



Metodi API LDAP

Element Software

NetApp
October 01, 2024

Sommario

- Metodi API LDAP 1
 - Trova ulteriori informazioni 1
 - AddLdapClusterAdmin 1
 - EnableLdapAuthentication 3
 - DisableLdapAuthentication 8
 - GetLdapConfiguration 9
 - TestLdapAuthentication 10

Metodi API LDAP

È possibile utilizzare il protocollo LDAP (Lightweight Directory Access Protocol) per autenticare l'accesso allo storage Element. I metodi API LDAP descritti in questa sezione consentono di configurare l'accesso LDAP al cluster di storage.

- [AddLdapClusterAdmin](#)
- [EnableLdapAuthentication](#)
- [DisableLdapAuthentication](#)
- [GetLdapConfiguration](#)
- [TestLdapAuthentication](#)

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"](#)

AddLdapClusterAdmin

È possibile utilizzare `AddLdapClusterAdmin` per aggiungere un nuovo utente amministratore cluster LDAP. Un amministratore del cluster LDAP può gestire il cluster utilizzando l'API e gli strumenti di gestione. Gli account amministratore del cluster LDAP sono completamente separati e non correlati agli account tenant standard.

Parametri

È inoltre possibile utilizzare questo metodo per aggiungere un gruppo LDAP definito in Active Directory®. Il livello di accesso assegnato al gruppo viene passato ai singoli utenti del gruppo LDAP.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
accesso	Controlla i metodi che l'amministratore del cluster può utilizzare.	array di stringhe	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AccetteEula	Accettare il Contratto di licenza con l'utente finale. Impostare su true per aggiungere un account amministratore del cluster al sistema. Se omissso o impostato su false, la chiamata al metodo non riesce.	booleano	Nessuno	Si
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
nome utente	Il nome utente distinto per il nuovo amministratore del cluster LDAP.	stringa	Nessuno	Si

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "AddLdapClusterAdmin",
  "params": {"username": "cn=mike
jones,ou=ptusers,dc=prodtest,dc=solidfire,dc=net",
  "access": ["administrator", "read"
  ]
},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {}
}
```

Novità dalla versione

9,6

Trova ulteriori informazioni

[Controllo degli accessi](#)

EnableLdapAuthentication

È possibile utilizzare il `EnableLdapAuthentication` metodo per configurare una connessione alla directory LDAP per l'autenticazione LDAP a un cluster. Gli utenti che sono membri della directory LDAP possono quindi accedere al sistema di storage utilizzando le proprie credenziali LDAP.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AuthType	Identifica il metodo di autenticazione dell'utente da utilizzare. Valori possibili: <ul style="list-style-type: none">• DirectBind• SearchAndBind	stringa	SearchAndBind	No
GroupSearchBaseDN	Il DN di base della struttura per avviare la ricerca della sottostruttura di gruppo.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
GroupSearchType	<p>Controlla il filtro di ricerca di gruppo predefinito utilizzato. Valori possibili:</p> <ul style="list-style-type: none"> • NoGroups: Nessun supporto di gruppo. • ActiveDirectory: Appartenenza nidificata a tutti i gruppi Active Directory di un utente. • MemberDN: Gruppi di stile MemberDN (livello singolo). 	stringa	ActiveDirectory	No
Server URI	<p>Elenco separato da virgole degli URI del server LDAP o LDAPS. È possibile aggiungere una porta personalizzata alla fine di un URI LDAP o LDAPS utilizzando i due punti seguiti dal numero della porta. Ad esempio, l'URI "ldap://1,2.3,4" utilizza la porta predefinita e l'URI "ldaps://1,2.3,4:123" utilizza la porta personalizzata 123.</p>	array di stringhe	Nessuno	Sì
UserSearchBaseDN	<p>Il DN di base della struttura per avviare la ricerca nella sottostruttura. Questo parametro è necessario quando si utilizza un AuthType di SearchAndBind.</p>	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SearchBindDN	Un DN completo con cui effettuare l'accesso per eseguire una ricerca LDAP per l'utente. Il DN richiede l'accesso in lettura alla directory LDAP. Questo parametro è necessario quando si utilizza un AuthType di SearchAndBind.	stringa	Nessuno	Sì
SearchBindPassword	La password per l'account searchBindDN utilizzato per la ricerca. Questo parametro è necessario quando si utilizza un AuthType di SearchAndBind.	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
UserSearchFilter	<p>Il filtro di ricerca LDAP da utilizzare quando si esegue una query sul server LDAP. La stringa deve avere il testo segnaposto "%USERNAME%" che viene sostituito con il nome utente dell'utente autenticante. Ad esempio, (&(objectClass=person)(sAMAccountName=%USERNAME%)) utilizzerà il campo sAMAccountName in Active Directory per corrispondere al nome utente immesso al momento dell'accesso al cluster. Questo parametro è necessario quando si utilizza un AuthType di SearchAndBind.</p>	stringa	Nessuno	Sì
UserDNTemplate	<p>Modello di stringa utilizzato per definire un modello per la costruzione di un nome distinto utente (DN) completo. La stringa deve avere il testo segnaposto "%USERNAME%" che viene sostituito con il nome utente dell'utente autenticante. Questo parametro è necessario quando si utilizza un AuthType di DirectBind.</p>	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
GroupSearchCustomFilter	Da utilizzare con il tipo di ricerca CustomFilter, un filtro LDAP da utilizzare per restituire il DNS dei gruppi di utenti. La stringa può contenere il testo segnato %USERNAME% e %USERDN% da sostituire con il nome utente e il nome utente completo in base alle necessità.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "EnableLdapAuthentication",
  "params": {
    "authType": "SearchAndBind",
    "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
    "groupSearchType": "ActiveDirectory",
    "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
    "searchBindPassword": "zsw@#edcASD12",
    "sslCert": "",
    "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
    "userSearchFilter":
    "(&(objectClass=person)(sAMAccountName=%USERNAME%))",
    "serverURIs": [
      "ldaps://111.22.333.444",
      "ldap://555.66.777.888"
    ]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
  }
}
```

Novità dalla versione

9,6

DisableLdapAuthentication

È possibile utilizzare questo `DisableLdapAuthentication` metodo per disattivare l'autenticazione LDAP e rimuovere tutte le impostazioni di configurazione LDAP. Questo metodo non rimuove gli account amministratore del cluster configurati per utenti o gruppi. Una volta disattivata l'autenticazione LDAP, gli amministratori del cluster configurati per l'utilizzo dell'autenticazione LDAP non possono più accedere al cluster.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DisableLdapAuthentication",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {}
}
```

Novità dalla versione

9,6

GetLdapConfiguration

È possibile utilizzare il `GetLdapConfiguration` metodo per ottenere la configurazione LDAP attualmente attiva sul cluster.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito.

Nome	Descrizione	Tipo
LdapConfiguration	Elenco delle impostazioni di configurazione LDAP correnti. Questa chiamata API non restituisce il testo normale della password dell'account di ricerca. Nota: se l'autenticazione LDAP è attualmente disattivata, tutte le impostazioni restituite sono vuote ad eccezione di "AuthType" e "groupSearchType", rispettivamente impostate su "SearchAndBind" e "ActiveDirectory".	LdapConfiguration

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetLdapConfiguration",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "ldapConfiguration": {
      "authType": "SearchAndBind",
      "enabled": true,
      "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
      "groupSearchCustomFilter": "",
      "groupSearchType": "ActiveDirectory",
      "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
      "serverURIs": [
        "ldaps://111.22.333.444",
        "ldap://555.66.777.888"
      ],
      "userDNTemplate": "",
      "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
      "userSearchFilter":
        "(&(objectClass=person)(sAMAccountName=%USERNAME%))"
    }
  }
}
```

Novità dalla versione

9,6

TestLdapAuthentication

È possibile utilizzare il `TestLdapAuthentication` metodo per convalidare le impostazioni di autenticazione LDAP attualmente abilitate. Se la configurazione è corretta, la chiamata API restituisce l'appartenenza di gruppo dell'utente testato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome utente	Il nome utente da verificare.	stringa	Nessuno	Sì
password	La password per il nome utente da verificare.	stringa	Nessuno	Sì
LdapConfiguration	Oggetto IdapConfiguration da testare. Se si fornisce questo parametro, il sistema verifica la configurazione fornita anche se l'autenticazione LDAP è attualmente disattivata.	LdapConfiguration	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
gruppi	Elenco dei gruppi LDAP che includono l'utente testato come membro.	array
Nome utente	Nome distinto LDAP completo dell'utente testato.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "TestLdapAuthentication",
  "params": {"username": "admin1",
            "password": "admin1PASS"}
},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "groups": [
      "CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
    ],
    "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
  }
}
```

Novità dalla versione

9,6

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.